Annual 47 CFR § 64.2009(e) CPNI Certification Template
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 26, 2019

2. Name of company(s) covered by this certification: Commercial Radio & Television, Inc.

3. Form 499 Filer ID: 812347

4. Name of signatory: Roger Combs

5. Title of signatory: Vice President

6. Certification:

I, Roger Combs, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company [*has not]* taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company [*has not]* received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Roger Combs

Attachments:
A: Accompanying Statement explaining CPNI procedures
B: Explanation of actions taken against data brokers
C: Summary of customer complaints

Attachment A

COMMERCIAL RADIO & TELEVISION, INC.
CUSTOMER PROPRIETARY NETWORK INFORMAITON
("CPNI") POLICIES AND PROCEDURES

---

1 Statement of Corporate Policy

The policy of Commercial Radio & Television, Inc. (the "Company) is to comply with the laws of the United States pertaining to Customer Proprietary Network Information ("CPNI") contained in §222 of the Telecommunications Act of 1996, as amended, and the FCC's regulations concerning CPNI. The Company's policy is to ensure that all levels of personnel properly learn, implement and enforce rules and regulations concerning CPNI. Pursuant to FCC regulations, the Company has implemented policies and procedures to ensure proper treatment of CPNI. All employees are required to learn and implement these procedures, or be subject to disciplinary action. This document constitutes the Company's policies and procedures related to CPNI.

The Company provides a primarily dispatch-only communications service, which some service is not interconnected with the public switched network, and is therefore classified by the FCC as Private Mobile Radio Service ("PMRS"), not Commercial Mobile Radio Service ("CMRS") These customers are not able to place or receive calls over the telephone network. Customers' two-way radios do not have telephone numbers and permit communications only with other employees of the same customer if their radios are so configured or with the customer's dispatcher.

Thus, the customer information to which the Company has access is not of the type that typically is considered CPNI or that might be expected to have value to any third party, thereby triggering the violations that the CPNI rules seek to prevent. Nonetheless, the Company recognizes that it is subject to the CPNI rules and has put in place the policies and procedures described herein to ensure its compliance with those requirements, including the policies and procedures that would be necessary should it interconnect its system and provide telephone numbers to its customers in the future

All employees are required to follow the policies and procedures described in this chapter.

2 Definition of CPNI

CPNI is information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information

contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information, which is subscriber names, addresses, phone numbers and/or advertising classifications that a carrier or its affiliate have published, or provided for publication, in a telephone directory.

Such information includes account numbers, the Company's telephone numbers, bill amounts, call records, minutes used, plan information, features information, locations or numbers called, equipment, and other account information. Employees unsure of whether requested information contains CPNI should ask their supervisors for guidance.

3 Use of CPNI

The Company does not provide or market categori*es of service besides* **PMRS and CMRS.** The Company may use, disclose, or permit access to CPNI without customer approval for the purpose of providing or marketing **PMRS and CMRS** service offerings, including the marketing of handsets and data or Blackberry services.

The Company does not use, disclose, or permit access to CPNI for marketing of any products not within the **PMRS and CMRS** category of service or adjunct thereto. Should the Company provide, market, or partner with another entity to market other categories of telecommunications service, these policies may be amended to reflect customer consent procedures consistent with state and federal law.

Prohibited Uses

The Company may not use, disclose, or permit access to CPNI to market non-commercial services, unless the customer has provided approval to do so (either opt-in or opt-out approval in accordance with FCC regulations). The Company may not use, disclose, or permit access to CPNI to track customer calls to competing service providers.

Permitted Uses

The Company may use CPNI to market **PMRS and CMRS** services, or services that are adjunct to basic wireless services (information services), including, but not limited to, speed dialing, directory assistance, call waiting, call forwarding, caller I.D., text messaging, wireless data, and Blackberry services.

The Company may also use, disclose, or permit access to CPNI, without customer approval, for the following:

1. To provide customer premises equipment (CPE).
2. To provide wiring, installation, maintenance, and repair services;
3. To research health effects of wireless service;
4. To protect the rights of the Company or to protect other users or carriers from fraudulent, abusive, or unlawful use of such services;
5. To create, calculate, bill, and collect for service; and,

6. To provide call location information (E911) concerning the user in an emergency.
7. In response to a law enforcement agency in accordance with applicable legal requirements.

4 Customer Authentication

The Company and its employees will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. All employees must properly authenticate a customer prior to disclosing CPNI during customer-initiated calls, online account access, or in-store visits.

Customer-Initiated Calls

"Call detail information" means any information pertaining to specific calls, including numbers called to/from, time, duration, or location of calls. *Amount of minutes used or remaining minutes of use are not call detail records.* When a customer calls a Company representative or authorized dealer, if any, the Company representatives may only disclose call detail information under the following circumstances:

1. If the customer gives his or her password, established online, if online customer care is used, or through the customer's account. The password may not use readily available biographical information such as addresses, SSN, or driver's license numbers. The representative may call the customer back at the wireless number associated with the requested records to establish a password for future call detail requests.

2. If the customer does not have a password, call detail information may be disclosed if the representative sends the information to the address on the customer account or by calling the customer back on the number associated with the requested records. Representatives may not call a different number to disclose information, and may not send the call detail records to any other address than that on the account.

3. If the customer is able to provide call detail information to the representative, then the representative may discuss the information provided by the customer.

Online Account Access (if applicable)

Online account access requires online authentication prior to disclosing CPNI. Such authentication will not use account information or readily available biographical information such as addresses, SSN, mother's maiden name or driver's license numbers.

In the event a customer forgets or loses the password, a back-up method may be used to authenticate a customer. The back-up method may not prompt the customer for account number or readily available biographical information.

In-Store and Dealer Inquiries

Retail sales associates and dealers, if any, may disclose CPNI to a customer, provided the customer presents a valid photo ID matching the customer's account information.

Business Customers

The Company may utilize other authentication procedures not described here for services provided to businesses, provided that the account has a dedicated account representative, and that the account has a contract specifically addressing the Company's protection of CPNI.

5 Notification of Account Changes

The Company will notify the customer via voicemail, text message, or US mail anytime a customer's password, response to back-up question, online account information, or address of record is created or changed. This notification is not required when the new customer initiates service, but is required when a current customer obtains a password online.

6 Notification of CPNI Security Breaches

A "security breach" has occurred if a person has intentionally gained access to, used, or disclosed CPNI without authorization.

In the event of a security breach, the Company's management will notify the United States Secret Service and the Federal Bureau of Investigation. Law enforcement notification will occur within seven (7) days of discovery of the security breach. The Company will not disclose the breach to the customer or the public until seven (7) days after law enforcement notification.

Once law enforcement has been notified and seven (7) days have passed, the Company will notify its customer[s] of the CPNI security breach. The Company will also keep electronic or other records of any breaches discovered, of law enforcement notifications, and of customer notifications for at least two (2) years.

7 Company Safeguards and Recordkeeping

Management Safeguards

Attachment A

1. Training of Company personnel and dealers, if any, with access to CPNI will include review of the CPNI policies and procedures herein for all new employees and all existing employees who have not previously gone through the training process. Additional training will be provided as-needed.

2. The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners, if any; (4) maintaining records regarding the use of CPNI in marketing campaigns, should that occur; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

   Company personnel will make no decisions concerning CPNI without first consulting the Compliance Officers: Roger Combs or Cary Rehm.

In deciding whether the Company use of CPNI is proper, the Compliance Officer will consult these policies, FCC regulations, and legal counsel as necessary.

3. In accordance with FCC regulations, the Compliance Officer will ensure that the Company enters into confidentiality agreements with partners or contractors to whom it discloses CPNI (for which it has received customer approval), in the event such disclosures are contemplated.

4. Files containing CPNI are maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

5. The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting, including requiring Company employees and agents to notify the CPNI Compliance Officer immediately to report any suspicious or unusual activities that might indicate pretexting efforts.

6. Any improper use of CPNI will result in disciplinary action in accordance with the Company's disciplinary policies. Violation of these policies and procedures will be treated as a serious offense, and may result in suspension or termination of employment.

7. On an annual basis, a Corporate Officer will sign a compliance certificate, to be filed with the FCC prior to March 1st, stating that he or she has

personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's rules.

Recordkeeping

1. The Company will maintain records of any sales and/or marketing efforts that use CPNI, including a description of each campaign and the products or services offered.

2. The Company will maintain records of all instances in which it discloses CPNI to third parties, including each campaign or project, the purpose of the disclosure, and the information disclosed.

3. All records concerning CPNI, including court orders concerning CPNI, will be maintained for a minimum of one (1) year in a readily available and identifiable separate file.

Attachment B

Commercial Radio & Television, Inc

Statement of Actions Taken Against Data Brokers

A. During Calendar Year 2018, the Company has instituted the following proceeding, or filed the following petitions. Against data brokers before the Federal Communications Commission: **NONE**

B. During Calendar Year 2018, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the state commission(s) having jurisdiction over it: **NONE**

C. During Calendar Year 2018, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the following federal or state courts: **NONE**

Attachment C

Commercial Radio & Television, Inc

Summary of Customer Complaints

Regarding Unauthorized Release of CPNI

A. During Calendar Year 2018, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by Company employees: **NONE**

B. During Calendar Year 2018. The Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information: **NONE**

C. During Calendar Year 2018, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information: **NONE**

D. During Calendar year 2018, the Company has become aware of the following processes that pretexters are using to attempt to access its CPNI: **NONE**